

Remarks/Arguments

Claims 9 - 16 are pending. New Claim 17 has been added to more fully claim the subject matter that applicants regard as their invention. No new matter is believed to be added by the present amendment.

Claims 9 - 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Friedman (United States Patent No. 5,499,294) in view of Caputo (United States Patent No. 5,778,071). Applicants traverse these rejections, and requests their reconsideration and removal for at least the following reasons.

Independent Claim 9 recites in relevant part a

“device for authenticating a user who takes pictures made up of digital data comprising a picture taking apparatus associated with detachable security elements, each detachable security element being specific to a user”.

The combined teachings of Friedman and Caputo fail to teach a device that authenticates a user who takes pictures – and hence, fails to render at least Claim 9 unpatentable.

As set forth in Applicants' amendment filed on November 1, 2004, the primary reference Friedman fails to even contemplate the problem addressed by the present invention, namely, that of authenticating a user who takes pictures. Friedman instead teaches a solution to an entirely different problem, namely that of authenticating the digital image taken from the picture taking device itself (or camera), and not a user of the device. See, e.g., *Specification, page 1, lines 14 – 28*.

The present Office action acknowledges this shortcoming of Friedman in that it admits “Friedman does not explicitly disclose that the security element comprises detachable security elements, each detachable security element being specific to a user.” *2/17/2005 Office Action, pg. 3, lines 3-4*. The Office action attempts to remedy this admitted shortcoming of Friedman by importing select portions of Caputo. In particular, the Office action argues

“Caputo discloses detachable security elements (smart cards) comprising a circuit associated with a secret key specific for that security element for signing digital data to give an encrypted output digital data; the detachable security elements being specific to a user.”

The Office action goes on to conclude,

“[a]t the time of invention, it would have been obvious to a person of ordinary skill in the pertinent art to modify the security element of Friedman, so that it comprises the detachable security elements of Caputo”.

In response, Applicants submit that even if one were to modify the system of Friedman to utilize the detachable security elements of Caputo, the suggested modification still fails to meet each of the limitations of Claim 9. Present Claim 9 recites:

Device for authenticating a user who takes pictures made up of digital data comprising a picture taking apparatus associated with detachable security elements, each detachable security element being specific to a user, and each detachable security element comprising a circuit associated with a secret key K1 specific to that security element and carrying out the signing of at least part of the digital data to give an encrypted output digital data, the security element being connected to the picture taking apparatus through an interface allowing a bi-directional transfer of data. (emphasis added).

The gist of the invention of Caputo is to prevent unauthorized access to communications networks and prevent eavesdroppers from reading proprietary data on communications lines. *See, e.g., U.S. Patent No. 5,778,071, Abstract; see also, col. 1, lines 10-21.* Specifically, in Caputo, device authentication is performed to ensure that a user who wishes to obtain access to communications equipment possesses an authorized device. The cited portions of Caputo merely include teachings directed to a smart card in general (col. 6, line 67 – col. 7, line 20) and to a device and user authentication scheme shown in Fig. 5B (col. 14, lines 23-57). The user authentication taught by Caputo is performed merely to indicate that the user of

a device knows a personal identification number (PIN) or password, in order to ensure that a stolen device may not be used. *See, U.S. Patent No. 5,778,071, col. 13, lines 4-13 (device authentication) and lines 14-24 (user authentication).*

Thus, even assuming *arguendo* that the combination of Friedman and Caputo is proper, modifying the Friedman scheme of digital camera authentication to include the user challenge scheme of Fig. 5B of Caputo to restrict unauthorized access to a stolen digital camera still fails to all of the limitations of present claim 9.

In fact, the referenced portions of Caputo are inconsistent with the recitation of Claim 9. Claim 9 recites *signing of at least part of the digital data (that makes up the pictures themselves) -- to give encrypted output digital data*. In contrast, the referenced portions of Caputo merely teach a challenge methodology in which a random number is generated that does not constitute payload data, the random number being supplied to a user portion, encrypted, and returned to and verified by the challenger portion. *See, e.g., U.S. Patent No. 5,778,071, Fig. 5B.*

Thus, importing the detachable security elements of Caputo, and even the device and user challenge scheme of Fig. 5B of Caputo, to the primary reference Friedman, would merely provide device and user authentication prior to permitting access to a digital camera that uses a public key unique to the digital camera system (rather than to a user) in order to authenticate digital images. *See, U.S. Pat. 5,499,294, col. 4, lines 30 – 46.* The above combination thus fails to teach the Claim 9 recitation of *signing at least part of the digital data making up pictures to give encrypted output digital data that authenticates a camera user*. For at least the foregoing reasons, the combination of Friedman and Caputo fails to teach each of the features and limitations recited in present claim 9; reconsideration and withdrawal of this 35 USC 103(a) rejection is requested.

The above notwithstanding, applicants submit that the proposed combination of Friedman and Caputo is improper, as no motivation exists for combining the references in the manner suggested absent impermissible hindsight gleaned from Applicants' own disclosure. There must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P.*

706.02(j)). In the instant case, Applicants submit it would be improper to modify the camera public key encrypted digital image data of Friedman, with the scheme depicted in Fig. 5B of Caputo, as Fig. 5B merely represents a device and user access challenge scheme, and not an encryption scheme. With regard to encrypting data once access is permitted by the referenced challenge scheme of Caputo (e.g., the scheme of Fig 5B results in a simple pass condition, *see, e.g., col. 14, lines 48-51*), Caputo merely teaches that any key may be used in accordance with a chosen algorithm, and that the choice of the encrypting/decrypting algorithm, and hence choice of key type, is unimportant to the Caputo invention. *See, e.g., U.S. Patent No. 5,778,071, col. 11, lines 2-3, 25 - 32.*

Furthermore, Caputo teaches a portable security device to be connected directly to telephone circuits to both authenticate an individual and encrypt data communications. *See, U.S. Patent No. 5,778,071, Abstract, lines 1-3.* Applicants submit this has little in common with, and addresses an entirely different problem (i.e. restricting network access) from the one which the primary reference seeks to address, namely authenticating digital images taken from a picture taking device (e.g. camera). In essence, Friedman authenticates picture taking devices while Caputo establishes secure communications across communications networks of varying protocols and standards. *See, U.S. Patent No. 5,778,071, col. 2, lines 61-64.*

The Office action argues Friedman and Caputo are "combinable" because they are both concerned with authentication systems that utilize secret keys for encrypting digital data. However, "the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination." *In re Mills, 916 F. 2d 680, 16 USPQ 2d 1430.* Applicants submit the cited art is devoid of any such suggestion.

Moreover, even assuming one would have been motivated to take advantage of Caputo's smart card environment, and further assuming one would have been motivated to incorporate the access restriction scheme of Fig. 5B of Caputo into Friedman, a proper motivation is still lacking for modifying Friedman's express teaching of authenticating a digital image taken from a

camera, with Caputo's encryption of a random number to restrict network access, in an attempt to reach the claim limitation of signing of at least a part of picture data to give an encrypted output file that authenticates a user.

The present invention adds a signature in a stream of digital image data using a detachable security device to allow one to recognize and authenticate the user of a camera or photographic apparatus. As previously discussed, Friedman fails to teach or suggest this approach. Caputo relates to encryption of random numbers (separate and apart from actual data to be transmitted and received via a communications network) to restrict unauthorized access to a communications network and also fails to teach the claimed approach. Accordingly, no combination of the cited references arrives at the invention as claimed in independent claim 9.

Accordingly, Applicants respectfully request reconsideration and removal of the rejection of Claim 9 for at least the aforementioned reasons. Applicants also request reconsideration and removal of the rejections of Claims 10 – 15, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 9.

In similar fashion to Claim 9 discussed above, independent Claim 16 recites

A system comprising a device for authenticating a user who takes pictures made up of digital data comprising a picture taking apparatus and a security element carrying out the signing of at least part of the digital data, the security element being a detachable element comprising a circuit associated with secret key K1, the detachable element and the associated secret key K1 being specific to a user.

For the reasons discussed above with regard to Claim 9, Applicants respectfully request reconsideration and removal of the rejection of Claim 16.

Newly added independent claim 17 recites the limitation that the encrypted output digital image data comprises signed data identifying the user. Support for this limitation may be found for example, on page 3 of the specification, in lines 19-39. The combined teachings of Friedman and Caputo fail to teach or suggest any circuit associated with a secret key K1 specific to that security element and carrying out the signing of at least part of the digital data to give an encrypted output digital data

CUSTOMER NO.: 24498
Serial No. 09/581,332
Final Office Action dated: 02/17/05
Response dated: 06/16/05

PATENT
PF970057
(RCA 90,215)


comprising signed data identifying the user. For at least these additional reasons, claim 17 is patentably distinct over the cited references of record and should be allowed.

CONCLUSION

Having fully addressed the Examiner's rejections, Applicants submit that the present application is in condition for allowance and respectfully request such action. No fee is believed due in regard to the present amendment. However, if a fee is due, please charge the fee to Deposit Account 07-0832. Should any questions arise regarding any of the above, the Examiner is requested to contact the undersigned at 609-734-6815.

Respectfully submitted,

SYLVAIN CHEVREAU ET AL.

By: 
Paul P. Kiel
Attorney for Applicants
Registration No. 40,677
(609) 734-6815

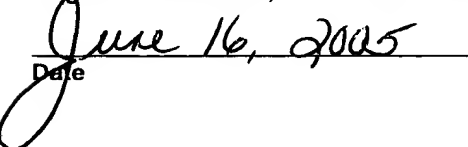
PPK:pdf

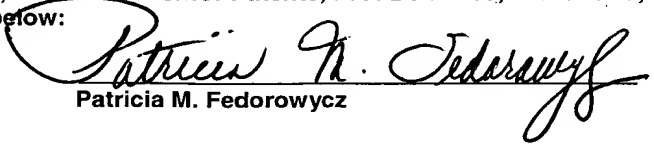
Patent Operations
THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

June 16, 2005

CERTIFICATE OF MAILING

I hereby certify that this correspondence (and any document referred to as being attached or enclosed) is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on the date indicated below:


Date


Patricia M. Fedorowycz